UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,293	04/04/2005	Mats Naslund	3995-42	4649

23117 7590 10/08/2010

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
10/08/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/530,293	**Applicant(s)** NASLUND ET AL.
	Examiner DARREN SCHWARTZ	**Art Unit** 2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2010 and 16 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *44,46 and 49-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *44,46 and 49-82* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *8-10-10 9-17-10*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

In view of the Pre-Appeal Brief filed on 21 July 2010, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

Claims 44, 46 & 49-82 are re-presented. Claims 63-78 stand as previously withdrawn. Claims 44, 46, 49-62 and 79-82 are presented for examination.

Response to Arguments

Applicant's arguments, see Pre-Appeal Brief, filed 21 July 2010, with respect to the rejections of the claims have been fully considered and are persuasive. In particular, arguments pertaining to Applicant's claimed cooperating application are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground of rejection is set forth *infra*.

To the extent Applicant's arguments may apply, the Examiner introduces Takahashi et al (U.S. Pat 6507907 B1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 44, 46, 49-59, 61 and 79-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wireless Identity Module," 12 July 2001, Wireless Application Protocol, WAP-260-WIM-20010712-a, hereinafter referred to as WIM, in view of Takahashi et al (U.S. Pat 6507907 B1), hereinafter referred to as Takahashi, in further view of Aura (U.S. Pat 6711400 B1), hereinafter referred to as Aura.

Re claim 44: WIM teaches a tamper-resistant security device (page 94: "13.2 WIM for Networks Not Utilizing a Smartcard Based SIM; In networks that do not utilize a smartcard based SIM, the WIM can be implemented ... in a tamper-resistant device, other than a smartcard") for use in a user device (page 8: "An example of a WIM implementation is a smart card. In the phone, it can be the Subscriber Identity Module (SIM) card or an external smart card.") comprising:

memory for storing user credentials, including at lest a security key associated with a user of the user device; an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key (page 8: "*The WAP Identity Module*

(WIM) is used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication. The functionality presented here is based on the requirement that sensitive data, especially keys, can be stored in the WIM, and all operations where these keys are involved can be performed in the WIM.");

a hardware communications interface for receiving one or more external AKA process commands from a device external to the tamper-resistant security device and returning processing results performed in the tamper-resistant security device in response to the one or more AKA process commands (Page 8: "The WAP Identity Module (WIM) is used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication. The functionality presented here is based on the requirement that sensitive data, especially keys, can be stored in the WIM, and all operations where these keys are involved can be performed in the WIM;" "An example of a WIM implementation is a smart card. In the phone, it can be the Subscriber Identity Module (SIM) card or an external smart card. The way which a phone and a smart card interact is specified as a command-response protocol, using Application Protocol Data Units (APDU) specific to this application. This specification is based on ISO7816 series of standards on smart cards and the related GSM specifications [GSM11.11], where applicable." page 17, section 6.1, ¶2-¶3; page 18, section 6.2.2).

However, WIM does not expressly disclose a cooperating application, contained within the tamper-resistant security device and having been given access rights to access the AKA module, configured to selectively receive the one or more AKA process commands and selectively provide enhanced security processing of the one or more AKA process commands.

Takahashi teaches a cooperating application [Fig 1A, elt 24; Fig 1B, elt 24; col 3, lines 12-15], contained within the tamper-resistant security device (col 3, lines 12-14; col 3, lines 19-22; *content is protected from unauthorized access or illegal copying*) and having been given access rights to access the AKA module [Fig 1A, elt 26; Fig 1B, elt 26; col 3, lines 15-18] (Fig 3A, elts 312—Yes→316; col 6, lines 23-29), configured to selectively receive the one or more AKA process commands (Fig 3A, elts 312, 316 & 318) and selectively provide enhanced security processing of the one or more AKA process commands (Fig 3B, elt 324; col 6, lines 37-42).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of WIM with the teachings of Takahashi, for the purpose of authenticating commands prior to granting access; it is known in the art that authentication preceding further actions preempts potential security issues.

The combination of WIM and Takahashi teaches an application interface internal to the tamper-resistant security device for interfacing said AKA module and said cooperating application so that the cooperating application performs the enhanced security processing in conjunction with the AKA module within the tamper-resistant security device (WIM: page 8: "An example of a WIM implementation is a smart card. In the phone, it can be the Subscriber Identity Module (SIM) card or an external smart card. The way which a phone and a smart card interact is specified as a command-response protocol, using Application Protocol Data Units (APDU) specific to this application This specification is based on ISO7816 series of standards on smart cards and the related GSM specifications [GSM11.11], where applicable." Takahashi: Fig 1A, elt 28; Fig 1B, elt 200, 202 & 28; col 6, lines 52-61; col 7, lines 42-45).

However, the combination of WIM and Takahashi does not expressly disclose wherein said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands.

Yet Aura teaches wherein said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module (Fig 4, elts 405 & 407; col 6, lines 39-49; col 7, lines 13-27) in response to the one or more AKA process commands (Fig 4, elts 401-404; col 6, lines 11-37), said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter (col 6, lines 40-62; col 6, line 66 – col 7, line 6) produced in response to the one or more AKA process commands (col 6, lines 11-37).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of WIM and Takahashi with the teachings of Aura, for the purpose of providing the known utility of protecting and validating the integrity of transmitted data via hash function.

Re claim 46: The combination of WIM, Takahashi and Aura teaches enhanced security processing includes pre-processing of at least one AKA input parameter (WIM: page 26: section 7.2.4.6; page 31: "Establishing pre-master secret;" Aura: col 2, lines 26-58).

Re claim 49: The combination of WIM, Takahashi and Aura teaches enhanced security processing includes evaluation of a predetermined number of consecutive AKA input parameters for verifying that said AKA input parameters can be used securely (WIM: page 18: "Signature verification by WIM may be used in cases where an application needs verification capability (e.g. certificate or end entity signature verification) but the verification algorithm is not present in the ME, or the verification algorithm implementation is more efficient in the WIM.").

Re claim 50: The combination of WIM, Takahashi and Aura teaches enhanced security processing further includes combination of a predetermined number of consecutive AKA output parameters generated in response to a number of corresponding unique AKA input parameters (WIM: see various APDU commands: pages 74-78).

Re claim 51: The combination of WIM, Takahashi and Aura teaches means for registration or detection of information representative of security conditions in relation to said tamper-resistant security device; and means for performing security policy processing based on said information (Takahashi: Fig 3, elements 306, 312, 320 and 324).

Re claim 52: The combination of WIM, Takahashi and Aura teaches the security conditions reflect at least one of an environment in which said security device is operated and a network interface over which a request for AKA processing originates (WIM: page 8: "The Wireless Application Protocol (WAP) is a result of continuous work to define an industry-wide specification for developing applications that operate over wireless communication networks.").

Re claim 53: The combination of WIM, Takahashi and Aura teaches security policy processing includes at least one of a security policy decision process and a security policy enforcement process (WIM: page 8: "This specification does not define exact requirements for tamper-resistance. Businesses can enforce certain requirements and policies using PKI based mechanisms. Applications should only accept certificates signed by Certification Authorities that are known to fulfill the requirements and policies.").

Re claim 54: The combination of WIM, Takahashi and Aura teaches means for performing security policy processing comprises means for selectively disabling direct access to said AKA module (WIM: page 95: "In a typical case, the PIN-G is used to protect all files (which need to be protected) and keys except non-repudiation keys. If the PIN-G is not disabled, the ME must send the PIN-G after the WIM application is selected, in order to be able to use keys and perform other operations that require the

PIN-G. More precisely, the ME SHOULD do the following when the secure functions are required the first time.").

Re claim 55: The combination of WIM, Takahashi and Aura teaches tamper-resistant security device comprises means for detecting whether said tamper-resistant security device is operated in its normal environment or in an environment considered insecure (WIM: page 49: "For the WAP-WTLS application there are two predefined SEs with their associated number."), and said means for performing security policy processing comprises means for disabling direct access to said AKA module when operated in said insecure environment (WIM: page 95: "In a typical case, the PIN-G is used to protect all files (which need to be protected) and keys except non-repudiation keys. If the PIN-G is not disabled, the ME must send the PIN-G after the WIM application is selected, in order to be able to use keys and perform other operations that require the PIN-G. More precisely, the ME SHOULD do the following when the secure functions are required the first time.").

Re claim 56: The combination of WIM, Takahashi and Aura teaches said cooperating application includes a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure (WIM: page 74, section 11.3.6.4: "PERFORM SECURITY OPERATIONS").

Re claim 57: The combination of WIM, Takahashi and Aura teaches cooperating application is performing at least part of the computations in connection with end-to-end key agreement between users (WIM: page 26, section 7.2.4.5: "WIM-KeyAgreement").

Re claim 58: The combination of WIM, Takahashi and Aura teaches cooperating application is masking key information generated by said AKA module (WIM: page 17: "The WIM is used to protect permanent, typically certified, private keys. The WIM stores these keys and performs operations using these keys;" page 18: "Application level security operations that use the WIM include signing and unwrapping a key").

Re claim 59: The combination of WIM, Takahashi and Aura teaches cooperating application is a software application installed in an application environment of said tamper-resistant security device (WIM: page 63: "The WIM application may have to reside on the card with other applications, eg, GSM. It is selected using an Application Identifier (AID) which is a combination of a Registered Application Provider Identifier (RID) and a Proprietary Application Identifier Extension (PIX) [ISO7816-5].").

Re claim 61: The combination of WIM, Takahashi and Aura teaches cooperating application is a privacy enhancing application, which participates in managing a user pseudonym (WIM: page 12: "A tamper-resistant device which is used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication.").

Re claim 79: The combination of WIM, Takahashi and Aura teaches said one or more AKA process commands include a random challenge [Aura: Fig 4, elts 401 & 404] and said at least one AKA output parameter [Aura: Fig 4, elt 405] includes a response to the random challenge that matches the random challenge (Aura: col 6, lines 30-49).

Re claim 80: The combination of WIM, Takahashi and Aura teaches said response is encapsulated using a function applied to manipulate the response to produce a higher security response (Aura: col 6, line 48 – col 7, line 6).

Re claim 81: The combination of WIM, Takahashi and Aura teaches said function is a keyed function (Aura: col 6, line 48 – col 7, line 6).

Re claim 82: The combination of WIM, Takahashi and Aura teaches said one or more AKA process commands include multiple random challenges [Fig 4, elts 401 & 404; see elements RAND1 & RAND2] and said at least one AKA output parameter includes multiple responses to the random challenges and said function is a keyed function of the multiple responses (Aura: Fig 4, elts 406, 407, 408 & 409; col 7, lines 13-46).

2. Claim 60 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wireless Identity Module," 12 July 2001, Wireless Application Protocol, WAP-260-WIM-20010712-a, hereinafter referred to as WIM, Takahashi et al (U.S. Pat 6507907 B1), hereinafter referred to as Takahashi and Aura (U.S. Pat 6711400 B1), hereinafter referred to as Aura, in further view of Vatanen et al (WO 00/48416), hereinafter referred to as Vatanen.

Re claim 60: The combination of WIM, Takahashi and Aura teach all the limitations of claim 59 as previously discussed.

However, Vatanen teaches said cooperating application is securely downloaded into said tamper-resistant security device from a trusted party (page 4, line 34 – page 5, line 3).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of WIM, Takahashi and Aura with the teachings of Vatanen, for the purpose of installing authenticate applications on a portable device. One of ordinary skill would recognize that installing authenticated software versus unknown software, prevents the spread of potential maleware or hostile software.

3. Claim 62 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wireless Identity Module," 12 July 2001, Wireless Application Protocol, WAP-260-WIM-20010712-a, hereinafter referred to as WIM, Takahashi et al (U.S. Pat 6507907 B1), hereinafter referred to as Takahashi and Aura (U.S. Pat 6711400 B1), hereinafter referred to as Aura, in further view of Miyoshi (U.S. Pat Pub 2003/0074570 A1), hereinafter referred to as Miyoshi.

Re claim 62: The combination of WIM, Takahashi and Aura teach all the limitations of claim 61 as previously discussed.

However, Vatanen teaches said privacy enhancing application is configured to request an AKA response from said AKA module based on an old user pseudonym and generate a new user pseudonym based on the received AKA response (Fig 5: elements

"RETURN TEMPORARY INTERFACE ID" and "DISTRIBUTE NEW REAL INTERFACE ID").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of WIM, Takahashi and Aura with the teachings of Vatanen, for the purpose of updating access control parameters; one of ordinary skill would recognize updating credentials prevents the potential illicit use of old credentials.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-5pm EST, Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435